UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/088,541	03/19/2002	Gary S Simpson	124-928	6928

23117 7590 01/31/2007
NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
BLUDAU, BRANDON S	
ART UNIT	PAPER NUMBER
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No. 10/088,541	Applicant(s) SIMPSON ET AL.
	Examiner Brandon S. Bludau	Art Unit 2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 November 2006*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-45* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This action is in reply to amendments filed 10/11/2006 and 11/03/2006. Claims 1-4,8,18-22,26,32,35,38,40,41, and 43 have been amended, Claims 44 and 45 are new claims and have been further amended in the submission on 11/03/2006. No claims have been cancelled, therefore claims 1-45 remain pending.

Claim Objections

2. Claim 1 is objected to because of the following informalities: in line 10, "providing for" should be indicated as an amendment. Appropriate correction is required.

3. Claim 38 is objected to because of the following informalities: line 10 reads "from said plurality thereof", this is referring to a plurality of levels, there is no antecedent basis for this in the claim.

Response to Arguments

4. Applicant's arguments filed 10/11/2006 have been fully considered but they are not persuasive. The Applicant argues that the Baker reference is not directed to individual human beings having access to datasets. The Applicant argues that Baker is only concerned with authorized terminals gaining access, not authorized users. The Examiner points to column 4 lines 36-46 in Baker to specifically point out wherein access is granted specifically to authorized users. Thus it is shown that Baker is in fact related to human user groups and is not restricted only to computer terminal user groups, contrary to that stated by the Applicant. Because it has been shown that Baker discloses human user groups, the Applicant's arguments pertaining to user group membership are also refuted by the Examiner (see the following rejections for

clarification). The Applicants arguments pertaining to authenticated evidence of membership are moot in view of the new grounds of rejection.

Claim Rejections - 35 USC § 103

5. Claims 1-5, 11-13,17,19-23,29,31,32,38, 41, 44 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baker (US Patent 5695898) and further in view of Davis et al. "An Implementation of MLS on a Network of Workstations Using X.500/509".

6. As per claim 1, Baker discloses a method for computer security to control access to data held on a computer system (columns 2,3 lines 66-3) as requestable datasets (see arguments above), said method comprising the steps of:

Allocating human users of a computer system between a plurality of user groups as members thereof, wherein not all user groups have only a single member and membership of a user group having multiple members is authentically evidenced by provision of user group identity information common to such members (column 4 line 65 – column 5 line 1, wherein the ID 207/208 is a single id that is common to users belonging to that user group), each user group corresponding to a respective dataset access category selected from a plurality of such categories such that all members of each user group having multiple members are associated with a dataset access category which is common to members of that user group (column 4 lines 36-46, 53-56 and column 5 lines 10-12 and 37-43);

Providing for each dataset a dataset access category selected from said plurality of such categories and associated with a criterion for access to that dataset by computer system users (column 4 lines 47-49 and 53-56 wherein the criterion for access is whether the user id is listed in the database as having access to the dataset); and

Giving access to a dataset to a member of a user group with multiple members in response to such member providing authenticated evidence of membership of that user group and members of that user group being associated with a common dataset access category which enables access to that dataset (column 4 lines 36-46 and 53-56).

Baker does not specifically disclose wherein the evidence of membership of the user group is authenticated evidence. The evidence discussed in Baker is an identification code, however Baker doesn't discuss how the identification code is authenticated. The Examiner notes that it is extremely common and well known in the art for access control systems to implement some method of authenticating a user identity. It would be obvious for one to modify Baker such that it included a step for authenticating the user identity for determining access privileges. Motivation as commonly understood, would simply be to ensure that the user is who he/she says he/she is. Moreover, Davis discloses a database system wherein the user identity is authenticated.

Davis however, does disclose wherein the identification means comprises authenticated evidence as can be clearly seen with the use of certificates see page 553 under heading B. titled: *Access Server Model.*

Davis is analogous art because it discusses a computer security system very similar to Baker.

It would have been obvious at the time of the invention for one of ordinary skill in the art to modify Baker to include a method of authenticating the identity of the system users.

Motivation for one of ordinary skill in the art at the time of the invention to modify Baker as discussed above would have been to "provide a framework of authentication services by the directory to its users" (Davis, page 548 under heading B). It can be understood by one of ordinary skill that the Baker architecture when developed in the directory structure would clearly necessitate an enhanced form of security offered by the certificate system.

7. As per claim 2, Baker discloses a method according to Claim 1, wherein user groups and data access categories have hierarchical levels in which a higher dataset access category incorporates a or, as the case may be, each lower data access category, and the method includes allowing access to datasets by members of user groups associated with dataset access category levels equal to and higher than those to which such datasets correspond (column 5 lines 6-12).

8. As per claim 3, Baker discloses a method according to Claim 1, wherein each user is associated with a computer based identifying means and the method includes the step of determining a user's identity from the identifying means (column 3 lines 54-56 and column 4 lines 36-39). Baker does not disclose wherein the identifying means is

a certificate means. Davis does include wherein the identifying means comprises the use of X.509 certificates. See the rejection to claims 1 and 4.

9. As per claim 4, Baker discloses all of the features of Claim 3, but does not disclose the use of X.509 certificates as the computer based identifying certificate means.

Davis discloses using a X.509 certificate as an authentication means for use in a conditional network access architecture on page 553 under heading B. titled: *Access Server Model*. .

Davis is analogous art because it discusses a computer security system very similar to Baker.

It would have been obvious at the time of the invention for one of ordinary skill in the art to modify Baker to include the use of X.509 certificates to identify the system users especially since Baker discusses using a tree structure format with directory and subdirectory listings and X.509 is the authentication framework for X.500 standard directories.

Motivation for one of ordinary skill in the art at the time of the invention to modify Baker as discussed above would have been to "provide a framework of authentication services by the directory to its users" (Davis, page 548 under heading B). It can be understood by one of ordinary skill that the Baker architecture when developed in the directory structure would clearly necessitate an enhanced form of security offered by the X.509 protocol.

10. As per claim 5, Baker discloses a method according to Claim 1, wherein datasets are web pages and the method includes the step of gaining access to the computer network via the Internet or the World-Wide-Web (column 2 line 3 – column 3 line 8).

11. As per claim 11, Baker discloses the data maintained on at least one database computer system (World Wide Web), and dataset access is given by access control software operated on a separate access control computer system (see Fig.1 block 112) and a user gains access to data by means of access request software running on a user computer system separate from the database and access control computer systems (see Fig. 1 blocks 107-109).

Baker does not explicitly state that the access control or the access request methods are on software, but one skilled in the art would clearly see that without explicitly saying software, the method that Baker discloses and implements must be run on and therefore inherently includes software at the user, access control, and database systems.

12. As per claim 12, Baker discloses a firewall at the access control system (see Fig. 1 block 113).

13. As per claim 13, Baker discloses the data is maintained on a plurality of database computer systems and in response to a data request, access control software determines whether or not corresponding data access is appropriate after relaying the request to a dataset computer system having such data (column 4 lines 7-15).

14. As per claim 17, Baker characterizes the step of giving access to a dataset includes unencrypted transfer of data from datasets to which access is granted (column

5 line 45; it is known to one of ordinary skill in the art that the http protocol includes unencrypted pages).

15. Claim 19 is rejected for disclosing the same subject matter as claim 1. One of ordinary skill in the art can clearly see that the method disclosed would inherently include a computer program so that it could be implemented.

16. Claim 20 is rejected for disclosing similar subject matter as claim 2.

17. Claim 21 is rejected for disclosing similar subject matter as claim 3.

18. Claim 22 is rejected for disclosing similar subject matter as claim 4.

19. Claim 23 is rejected for disclosing similar subject matter as claim 5.

20. Claim 29 is rejected for disclosing similar subject matter as claim 12.

21. Claim 31 is rejected for disclosing similar subject matter as claim 17.

22. Claim 32 is rejected for disclosing similar subject matter as claim 1, wherein the network access controller is found in Baker (Fig 1 number 112).

23. As per claim 38, Baker discloses a method for controlling user access to data held on a computer system as requestable datasets, the method including:

Labeling the datasets with dataset access labels defining a hierarchy of data access levels each associated with a criterion for access to a dataset by computer systems users,

Allocating human users of a computer system between a plurality of user groups as members thereof wherein not all user groups have only a single member and membership of a user group having multiple members is authentically evidenced by provision of user group identity information common to such members, Labeling user groups with data access levels selected from said plurality thereof such that all members of each user group having multiple members are associated with a dataset access level which is common to members of that user group; and

Giving access to a requested dataset to a requesting member of a user group with multiple members in response to such member providing authenticated evidence of membership of that user group and members of that user group being labeled with a common data access level which in the hierarchy is equal to or above the dataset access level of the requesting dataset (see rejections to claims 1 and 2 wherein there is an implied labeling of the data set access categories as discussed in Baker).

24. Claim 41 is rejected under similar arguments as claims 32 and 38.

25. Claim 44 is rejected under similar arguments as applied to the rejections of claims 1 and 2.

26. Claim 45 is rejected under similar arguments as applied to the rejections of claims 1-3.

27. Claims 6,24,39 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baker and Davis as applied to claim 3 above, and further in view of Hsiao et al. (US Patent 6496944).

28. As per claim 6, Baker discloses that the datasets are web pages, but does not disclose that the step of associating each dataset with a dataset access category comprises inserting meta tags in html web page code.

Hsiao discloses wherein meta data of a database entry comprises dataset access categories (column 5 lines 39 –42 wherein the security attributes and the access control list serve as the associating access information). Hsiao is directed to a method of assisting database system restore, which the Examiner acknowledges is not analogous art. However, the Examiner notes that it is well known and practiced in the art to associate meta data with tags on documents to be stored in a database system. Typically the meta data for documents contains information about the size, type, author, summary etc. Hsiao discloses that the meta data for documents can also include security parameters and access control lists. It would also be obvious for one of ordinary skill in the art to see the parallels with meta tags on documents directed to access control in a database system and html meta tags to control access to pages on the Internet, thus making the argument analogous.

Motivation for one of ordinary skill in the art to modify Baker to include associating the dataset access categories with meta tags in html web page code, would be the same as is used in the database systems wherein it is more efficient and practical to identify an access category in the meta data of each entity, than to place all entities in category lists as would be well known by one of ordinary skill and as is practiced prevalently in the art.

29. Claim 24 is rejected because it is directed to similar subject matter as claim 6.

30. As per claim 39, Baker discloses a method according to claim 38 wherein the datasets are web pages with data access levels, and a proxy server is used to:

Receive requests for web pages from members of user groups,

Check user group data access levels against a prearranged access control list, and

Deny members of a user group access to requested web pages if they lack a data access level appearing on the access control list (column 3 lines 8-15).

Baker does not disclose wherein the labels are meta tags.

Hsiao discloses the use of meta tags as described above in the rejection for claim 6. The same argument holds for the rejection of claim 24.

31. Claim 42 is rejected because it discloses similar subject matter as claim 39.

32. Claims 7 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baker and Davis.

33. As per claim 7, Baker discloses the method of claim 1, but does not disclose the method further including the step of performing a challenge-response exchange regarding user identification before the step of giving access to a dataset.

Baker uses id codes to identify the user, but it is not discussed how the user is authenticated. The Examiner notes that challenge-response exchanges are extremely common and well known in the use of user authentication for a variety of systems.

Therefore it would be obvious for one of ordinary skill in the art to modify Baker to use a challenge-response identification scheme for authenticating the user.

Motivation for one to modify Baker would be to enhance the security of the identification step as would be understood by one of ordinary skill in the art. Most challenge–response methods use some sort of token or key to generate a unique response to a challenge, thus precluding one from having their credentials intercepted over the network and preventing a re-use attack on the system as is common understood in the art.

34. Claim 25 is rejected for disclosing similar subject matter as claim 7.

35. Claims 8,9, 26 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baker, Davis and further in view of Harn "ID-Based Cryptographic Schemes for User Identification, Digital Signature, and Key Distribution".

36. As per Claim 8, Baker discloses a method according to Claim 1 in which a user group member employs a user computer system to gain access to datasets to which access is controlled by an access control computer system, but does not disclose wherein that computer system has a public key for verifying signed data, wherein each user computer system incorporates a private key for signing data and user group identifying means, and the dataset access step includes:

Using the private key to sign test data provided by the access control computer system and forwarding the signed data and user group identity information provided by the identifying means to the access control computer system; and

Using the access control computer system to;

verify the user group identity information, verify the user by using the public key to verify the signed data, and determine user group and associated dataset access category from the user group identity information.

Harn discloses a scheme, wherein "user identification can be achieved directly through a challenge-response type procedure." The steps of the scheme include using a private key to sign test data (wherein the data is a randomly selected odd number) provided by the access control computer system and forwarding the signed data and identifying means to the access control computer system; and using the access control computer system to verify the identifying means, verify the user by using the public key to verify the signed data, and determine user group and associated data access category from the identifying means (page 758). It would be obvious for one of ordinary skill in the art to see that the user group and data access category information, while not explicitly stated, could be included in the identification data.

Harn is analogous art to Baker, as it pertains to authentication and identification schemes for identification in a network system.

It would have been obvious at the time of the invention to modify Baker to include a more robust identification scheme using the public key authentication method, as public key cryptography is a widely known and used method of authenticating users to computer systems.

Motivation for one of ordinary skill in the art at the time of the invention to modify Baker as discussed above would be to "provide user identification and digital signature" and to establish a secure and secret communication session as taught in Harn (page 757) and as would be understood by one of ordinary skill in the art.

37. As per claim 9, Baker and Harn disclose claim 8 as discussed above, wherein Harn discloses the test data is random data (page 758).

38. Claim 26 is rejected for disclosing similar subject matter as claim 8.

39. Claim 27 is rejected for disclosing similar subject matter as claim 9.

40. Claims 10,28,34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baker and Davis as applied to claim 1 above, and further in view of McNabb (US Patent 6,289,462).

Baker discloses the method of claim 1 while Davis discloses providing database access to a first kind of user having a user certificate for identification purposes.

Neither Baker nor Davis discloses granting database access to a second kind of user lacking a user certificate.

McNabb discloses allowing database access to unauthorized users as anonymous access (column 18 lines 5-7 lines and column 22 lines 44-46). While McNabb doesn't explicitly describe an authentication method using certificates, one of ordinary skill in the art could easily see that the authorization method in McNabb could be performed with user certificates.

It would have been obvious for one of ordinary skill in the art to modify Baker and Davis to include a step of authentication to a user lacking a user certificate.

McNabb is analogous art because it relates to a security method that grants access privileges based on security-level attributes, with a similar access control structure as discussed in Baker.

Motivation for one of ordinary skill in the art to modify Baker/Davis to include access for users without certificates would be to allow access to public or non-sensitive data held on the database as implied in McNabb.

41. Claim 28 is rejected for disclosing similar subject matter as claim 10.

42. Claim 34 is rejected for disclosing similar subject matter as claim 10.

43. Claims 14-16, 30 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baker/Davis as applied to claim 1, and further in view of Hayman (US Patent 5,859,966).

44. As per claim 14, Baker discloses the method of claim 1, but does not disclose that the data access categories and the user groups and datasets with which they are associated are assigned numerical values.

Hayman does disclose that numerical values are assigned to the data access categories and the user groups and datasets with which they are assigned (column 8 line 16-18) and inherently explains the step of giving dataset access involves comparing user group and dataset numerical values to determine whether or not access is to be granted or denied. It is not an object of Hayman's invention to assign numerical numbers, but Hayman references mandatory access protocol (MAC) as described in the specification of the applicant wherein the MAC labels are stored as numeric values.

It would be obvious for one of ordinary skill in the art to modify Baker to include assigning numerical values to access categories.

Motivation for one of ordinary skill in the art to modify Baker as discussed above would have been to simplify the categorization of data objects by assigning them access numbers instead of having to arrange access lists as could be easily deduced by one of ordinary skill in the art.

45. As per claim 15, Hayman discloses that the data access categories have different sections each with a section numerical value and the step of comparing numerical values comprises comparing section numerical values of corresponding sections of user group and dataset numerical values (column 8 line 16-18 wherein the sections are referred to as categorical components).

46. As per claim 16, Hayman discloses that access to a dataset is provided only if all section comparisons are satisfied (column 8 39-45).

47. Claim 30 is rejected for disclosing similar subject matter as claim 14.

48. Claim 33 is rejected for disclosing similar same subject matter as claim 14.

49. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Baker/Hayman as applied to claim 16 and further in view of Netscape (Netscape Messaging Server Version 3.0 Administrator's Guide, Netscape Communications Corporation, 1995 pages 57-58).

Baker and Hayman disclose the method according to claim 16 as discussed above.

Baker and Hayman do not disclose the step of running checking/blocking software on the user computer system to screen incoming data for encryption to block unwanted data content.

The Administrator's Guide discloses an SSL package that allows the user to configure a specific port to block encrypted data.

The Administrator's Guide is analogous art because it relates to how data is handled over a network and Baker discloses a network that as typically found in the art supports SSL for secure data transfer. Therefore it would have been obvious for one of ordinary skill in the art to modify Baker to include the blocking software, as this is a well-known feature in data networks.

Motivation for one of ordinary skill in the art at the time of the invention to modify Baker-Hayman to include blocking software would be to allow the user the ability to specify the level of encryption for receiving and managing data as taught in Netscape page 57.

50. Claim 35 is rejected under 35 U.S.C. 103(a) as being unpatentable over Baker as applied to claim 19 and 32 above, and Davis as applied to claim 4. Wherein the computer network for database access is that which is shown in Baker, Fig.1.

51. Claim 36 is rejected under similar arguments as claim 6.

52. Claim 37 is rejected under similar arguments as claim 5.

53. Claims 40 and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baker as applied to claims 1 and 2, Davis as applied to claim 4, and Harn as applied to claim 8.

54. As per claim 40, Baker discloses a method for controlling access to data held on a computer system as requestable web pages (claim 1), the method including:

Allocating human users of a computer system between a plurality of user groups as members thereof wherein not all user groups have only a single member and membership of a user group having multiple members is authentically evidenced by provision of user group identity information common to such members,

Labeling user groups with respective data access levels associated with member groupings and selected from said plurality thereof such that all members of each user group having multiple members are associated with a dataset access level which is common to members of that user group (claim 1),

Using a proxy server to:

Receive a request for a web page from a client computer system having web browser software and client proxy software and controlled by a requesting member of a user group, and

Give access to a requested web page to the requesting member if said requesting member is a member of a user group with multiple members in response to such member providing authenticated evidence of membership of that user group and members of that user group being labeled with a common data access level in which the hierarchy is equal to or above the dataset access level of the requested web page (claim 2).

Baker does not disclose:

Labeling the web pages with meta tags defining a hierarchy of data access levels for an access control list providing a plurality of data access levels each associated with a criterion for access to a dataset by computer system users.

However, in view of claim 6 and claim 38, the examiner applies the same argument in deducing obviousness for one to apply meta tags with the security access level comprised therein to the datasets in Baker (see claims 6 and 38).

Baker does not disclose wherein each member has a key for signing data and a certificate indicating groupings to which that member belongs and wherein the proxy server:

sends data for signature to the client computer system and obtain the requesting member's certificate,

receives data from the client computer system, verifies that the received data is:

signed with the requesting member's key,

a signed equivalent of the data sent to the requesting member for signature, and

signed with a key from a certificate which is not time expired or invalid, and

if the received data is verifies as aforesaid, check the data access level of the requesting member's user group against the access control list.

Harn and Davis combined do teach these limitation, wherein as applied in claim 4, Davis teaches the use of user certificates for gaining access and recognizing users in a multi-level security protocol and Harn as applied in claim 8, discusses the well known method of challenge response user authentication. The rejections to claims 4 and 8 are applied herein, and one of ordinary skill in the art would be able to see the motivation and obviousness of combining these methods with Baker, as Harn and Davis discuss common features in database access and access control systems. Motivation, as would easily be deduced by one of ordinary skill, is to increase the security and authentication stages by requiring user certificates and private keys for challenge response identification.

55. Claim 43 is rejected because it discloses similar subject matter to claim 40.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Bludau whose telephone number is 571-272-3722. The examiner can normally be reached on Monday -Friday 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Brandon S Bludau
Examiner
Art Unit 2132

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100